Public Safety Spectrum Trust

1101 K Street, NW, Suite B100
Washington, DC 20005
www.psst.org

June 23, 2008

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, WT Docket No. 96-86

Dear Ms. Dortch:

Attached please find an amended copy of Attachment C ("Shared Wireless Broadband Network Technical Analysis") to the Comments filed by the Public Safety Spectrum Trust Corporation ("PSST") on June 20, 2008. It has come to our attention that the previously filed copy included a couple of clerical errors. We submit the attached corrected copy for the record. This revised Technical Analysis has also been posted on the PSST's website.

Respectfully submitted,

/s/ Harlin R. McEwen

Harlin R. McEwen
Chairman
Public Safety Spectrum Trust Corporation
Suite B100
1101 K St., NW
Washington, D.C. 20005

ATTACHMENT C

Shared Wireless Broadband Network

Technical Analysis

June 23, 2008

Table of Contents

I. Overview

The Public Safety Spectrum Trust Corporation ("PSST"), the Public Safety Broadband Licensee ("PSBL") for the 700 MHz public safety broadband spectrum, submits the following discussion of public safety expectations for the technical parameters and capabilities that should be required of the Shared Wireless Broadband Network ("SWBN").

II. Specifications for Public/Private System Architecture

A. FCC Rule

§ 27.1305 (2)(a) / § 90.1405 (2)(a)

The SWBN developed by the 700 MHz Public/Private Partnership between the PSBL and the D Block licensee and constructed by the D Block licensee must be designed to meet the requirements associated with a nationwide public safety broadband network. At a minimum, the SWBN must incorporate the following features:

1. Design for operation over a broadband technology platform that provides mobile voice, video, and data capability that is seamlessly interoperable across local and state public safety agencies, jurisdictions, and geographic areas, and that includes current and evolving state-of-the-art technologies reasonably made available in the commercial marketplace with features beneficial to the public safety community (*see* Sec. II below).
2. Sufficient signal coverage to ensure reliable operation throughout the service area, consistent with typical public safety communications systems (*see* Sec. VI below).
3. Sufficient robustness to meet the reliability and performance requirements of public safety (*see* Sec. III below).
4. Sufficient capacity to meet the day-to-day and emergency needs of public safety (*see* Sec. IV below).
5. Security and encryption capabilities consistent with state-of-the-art technologies (*see* Sec. V below).
6. A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis, consistent with the requirements of § 27.1307 (*see* Sec IV.D below).
7. Operational capabilities consistent with the features and requirements that are typical of current and evolving state-of-the-art public safety systems (*see* Sec. VII below).
8. Operational control of the network by the PSBL to the extent necessary to ensure that public safety requirements are met (*see* Sec. VIII below).

B. PSST SWBN Technology Platform Expectations

1) The technology selection and upgrade and migration plans will be the decision of the D Block operator, subject to PSST approval. Multiple open standards technologies that meet public safety requirements are viable.
2) The SWBN technology platform will be based, wherever possible, on commercial off-the-shelf (COTS) technology that provides mobile data, video, and cellular voice capabilities that are seamlessly interoperable across agencies, jurisdictions, and geographical areas.
3) The SWBN technology platform should provide cellular Push-To-Talk (PTT) capability to be used as a back-up for mission-critical land mobile radio networks. The preference is to have the cellular PTT capability available at network launch.
4) The SWBN technology platform will use a single common air interface (CAI) and the CAI must allow for a migration to future technology upgrades.
5) The technology selected for the SWBN will evolve and be upgraded based on commercial wireless upgrade timeframes; however, future upgrades should be backward–compatible, allowing for appropriate transition periods so that devices used by public safety entities do not become obsolete prematurely.
6) The PSST and the D Block winner will establish a joint program to identify public safety user requirements affecting the network technology road map and will support the appropriate standards development organizations' (SDOs') processes to encourage those requirements be included in subsequent technology releases.
7) The SWBN should launch with and/or upgrade to within a reasonable period, a uniform, IP Version 6 as required based on Federal government mandates.
8) During normal conditions, public safety users will have assured priority access on up to 50% of the engineered SWBN site capacity. During emergency conditions, public safety users will have assured priority access on up to 70% of the engineered SWBN site capacity.
9) During both normal and emergency conditions, the SWBN should support pre-emption of public safety users over commercial users on up to 50% of the engineered SWBN site capacity.

III. Reliability, Robustness, and Hardening

A. FCC Rule

§ 27.1305 (2)(c); § 90.1405(2)(c)

Sufficient robustness to meet the reliability and performance expectations of public safety.

Second R&O Para 405

Sufficient robustness to meet the reliability and performance expectations of public safety. To meet this standard, network specifications must include features such as hardening of transmission facilities and antenna towers to withstand harsh weather and disaster conditions, and backup power sufficient to maintain operations for an extended period of time.

B. PSST Network Reliability, Availability, and Hardening Expectations

1) To meet public safety expectations for mission-critical communications, the SWBN must be usable during extremely adverse operational and weather conditions. The higher the level of communications reliability and availability, the more effectively public safety users can execute their jobs during the most critical times. The goal is to construct a highly reliable and available network that is better than commercial wireless networks today, yet economically viable. This can be achieved through a variety of means such as hardening the terrestrial network, strategic storage staging and use of emergency deployable infrastructure and backup reliance on satellite coverage.
2) The RF signal level reliability is expected to be 95% over 95% of the area covered. The RF link is not included when calculating the availability numbers that follow.
3) The SWBN is expected to provide 99.9% availability at Year One of operation (calculated on jurisdictional boundaries). The exact method for measuring availability will be negotiated as part of the Network Sharing Agreement ("NSA"); however, the intent is for this to be a measure of infrastructure availability as measured from the antenna back through the core network and will exclude scheduled maintenance downtime as coordinated with the PSST.
4) SWBN specifications must include commercial best-practices, which take into consideration local influencing factors such as weather, geology, and building codes on network attributes such as hardening of transmission facilities and antenna towers, extended backup power, seismic safety standards, and accommodations for wind, ice and other natural phenomenon.
5) The SWBN cellular-like network architecture obviates the need for economically non-viable reliability and availability measures (as a requirement for extended power and redundant backhaul at every site, such as might be the case for traditional public safety high-site, high-power systems without overlapping coverage). However, sites designated as "critical" must have battery backup power of 8 hours and

generators with a 5 to 7- day fuel supply. Some sites will require redundant backhaul to meet the network availability standard.

6) The designation of a site as “critical” shall be a joint decision by the D Block operator, the PSST, and local public safety agencies, with a limitation that critical sites shall not exceed 50% of the operational SWBN site count. The use of emergency deployable infrastructure will be factored into the overall network availability measurement.

IV. Network Capacity

A. FCC Rule

§ 27.1305(2)(d); § 90.1405(2)(d)

Sufficient capacity to meet the needs of public safety.

Second R&O Para 405

Sufficient capacity to meet the needs of public safety, particularly during emergency and disaster situations, so that public safety applications are not degraded (*i.e.*, increase blockage rates and/or transmission times or reduced data speeds) during periods of heavy usage.

B. PSST Network Capacity Expectations

1) The SWBN must have sufficient capacity to meet identified needs of public safety in everyday normal operations as well as during unusual events or emergencies. PSST analysis concludes that the 20 MHz SWBN employing a 10 x10 MHz channel via an advanced 4G wireless broadband technology can provide sufficient capacity to make the network commercially viable, and meet public safety user needs under normal operations and emergency conditions.
2) To facilitate capacity and forecast planning, the D Block operator should provide the PSST monthly with summary and detail priority user utilization data. Both the PSST and the D Block operator will jointly forecast priority user demand and capacity needs.

C. FCC Rule

§ 27.1305(2)(f); § 90.1405(2)(f); § 27.1307

A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis consistent with the requirements of [§ 27.1307] and 90.1407(c).

Second R&O Para 405

A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis and to assign the highest priority to communications involving safety of life and property and homeland security consistent with the expectations adopted in this Second Report and Order.

D. PSST Public Safety Priority and Quality of Service (QoS) Expectations

The technology deployed on the SWBN will determine the specific method used to provide network priority and QoS to meet the PSST's priority and QoS expectations. Within all current advanced broadband technologies, varying levels of capabilities exist to provide degrees of priority and QoS management. Consistent with the FCC requirements, the PSST will have overall responsibility for assignment of the highest levels of network priority and QoS to public safety and other PSST-approved priority users.

a) Priority

1) Priority will be defined as PSST-approved user, network, application, and services priorities that, via user and/or device identification, offer the highest assignable levels of priority for network access and use of network resources, services, and applications.
2) Public safety and other PSST-approved priority users will be provided priority service that will allow for different levels of service priority, based on the given role of a user.
3) The highest 50% of access priority levels available in the radio access network technology will be allocated for assignment and use only for PSST-approved public safety and other users.
4) In the event that SWBN bandwidth is congested due to commercial use, the network will provide an automatic mechanism to accommodate public safety users by pre-empting commercial users and providing public safety users up to 50% of the site engineered capacity.
5) Under normal conditions, the network will provide assured priority access to public safety users on up to 50% of the site engineered capacity. During emergency conditions, the network will provide assured priority access to public safety users on up to 70% of the site engineered capacity.
6) The SWBN will provide an appropriate priority to 9-1-1 calls per applicable FCC requirements; 9-1-1 calls would not be subject to pre-emption.

b) Quality of Service (QoS)

1) The determination of QoS classes is technology-dependent, but it is anticipated that the SWBN will support up to 7 defined classes of service.
2) QoS will refer to resource reservation and session control mechanisms.
3) QoS mechanisms will provide different levels of performance to a traffic/data flow in accordance with predefined class of service and its associated performance parameters for identified applications and/or services.
4) QoS will be considered the full class of mechanisms that are found at multiple IP layers in the network (both RAN and Core) to provision and apply priority for IP packet-based traffic.
5) The assignment of network resources will take into account the user and/or service priority as well as the QoS requirements of the application.
6) The SWBN will support multiple QoS flows between a user device and network, where each flow may have a different QoS requirement and priority level.

7) If network resources are not available to meet a resource reservation request, the SWBN should have the ability to negotiate a mutually acceptable QoS with the user device.
8) All PSST priority user logical client-based VPN and layer 2/3 Virtual Private Network (VPN) will be configured and provisioned within the SWBN to have the highest authorized IP packet routing and queuing treatment.
9) The methods by which QoS will be promulgated across the SWBN will be dependent on the technology employed. Therefore, the PSST expects that the D Block winner will coordinate with the PSST to identify and document the configuration parameters for the chosen SWBN technology required to provide the specified QoS for PSST-authorized or PSST-designated services, applications, and permissions.

V. Security and Encryption

A. FCC Rule

§ 27.1305(2)(e); § 90.1405(2)(e)

Security and encryption consistent with state-of-the-art technologies.

B. PSST Network Security and Encryption Expectations

1) The SWBN should accommodate compliance with FBI Criminal Justice Information System (CJIS) guidelines, which include physical security guidelines, advanced authentication methods, and unique identifiers for authenticated users. Standards for network security also will be complied with and incorporated.
2) The SWBN should accommodate compliance with the National Information Exchange Model (NIEM) to facilitate the sharing of emergency and incident information across agencies and jurisdictions.
3) The SWBN should implement controls to ensure that public safety priority and secure network access is limited to authorized public safety users and devices.
4) The SWBN should utilize an open standard protocol for authentication.
5) Some of public safety's unique needs are not provided for in a commercial service context. The SWBN should allow for public safety network authentication, authorization, automatic logoff, transmission secrecy and integrity, and audit control capabilities, as well as other unique attributes.
6) There should be a joint effort by the PSST and the D Block licensee to introduce into commercial technology standards bodies the security and encryption and other functional specifications that are needed by public safety.
7) PSST recommendations for data and operations security safeguards and controls should be incorporated into the D Block licensee's data security policies and procedures.

VI. Coverage

A. FCC Rule

§ 27.1305(2)(b); § 90.1405(2)(b); § 27.14(m)(1)

Sufficient signal coverage to ensure reliable operation throughout the service area consistent with typical public safety communications systems.

B. PSST Proposed Coverage Requirements

The FCC could consider alternative approaches, such as the following example, to balance the needs of public safety against the D Block licensee's legitimate cost concerns:

YEAR	% OF TOTAL POPULATION
4	75%
7	95%
10	98%
15	99.3% The PSST desires to achieve long-term 99.3% coverage

The population requirement includes coverage of communities in excess of 3,000 people are part of the build-out, as well as all major US highways and interstates.

With PSST approval and device availability, satellite and roaming agreements may be used to calculate population coverage.

C. PSST SWBN Coverage and RF Reliability Expectations

1) It is expected that signal levels will be sufficient to provide the RF reliability defined in Table I-A (below) to ensure coverage consistent with public safety operational requirements.
2) To promote SWBN usage, the D Block operator and PSST will review the build plan and progress, and jointly adjust it to provide coverage in difficult areas. This activity will occur as part of network capacity and forecasting coordination already discussed in Section IV, paragraph B(2).

D. PSST Signal Reliability Expectations

1) The SWBN should provide seamless coverage (via handoff/handover mechanisms) and continuous connectivity with a 95% signal level reliability over 95% of an area as defined by county, township, or parish boundaries at stationary and vehicular speeds up to 75 miles per hour (120 km/h).
2) Published originally in the NPSTC Broadband Working Group's Statement of Requirements (SoR)[1], Table I-A (below) is provided to assist in determining average cell site radii per morphology class.
3) Table I-A also represents anticipated data rates through the first 4 years of operation, anticipating commercial standard improvements as the network build plan progresses.

Table I-A Propagation and Capacity Parameters

Morphology	*In-Building Penetration Margin*	*Coverage Availability*	*Sector Loading* Sector is loaded to this level of traffic	*Forward Link Throughput* •**On-street** •**Single user** • Average cell edge throughput	*Reverse Link Throughput* • **On-street** • **Single user** • Average cell edge Throughput
Dense Urban	22 dB	95%	70%	1000 kbps	256 kbps
Urban	19 dB	95%	70%	1000 kbps	256 kbps
Suburban	13 dB	95%	70%	512 kbps	128 kbps
Rural	6 dB	95%	70%	512 kbps	128 kbps
Highway	6 dB	95%	70%	128 kbps	64 kbps

[1] Public Safety 700 MHz Broadband Statement of Requirements

Table I–B Morphology Class Parameters

Morphology	*Population Density Based on County Boundaries (pops/sq mile)*	*Area Description*	*Approximate Land Mass* (sq mile)
Dense Urban	+15,000	Skyscrapers, high rise apartments, buildings of 20+ stories, narrow streets	297
Urban	2,500 – 14,999	Hotels, hospitals, buildings of 4-19 stories, medium to narrow streets	12,367
Suburban	200 – 2,499	Buildings of 1-3 stories, trees and foliage, medium width streets	258,380
Rural	0 – 199	Large open spaces, isolated highways, 1 -2 story houses, barns	3,268,719
Highway	NA	Stretches of interstate highway, and/or US highways, principally within under-populated areas	NA

VII. Operational Capabilities – Network Services and Applications

A. FCC Rule

§ 27.1305(2)(g); § 90.1405(2)(g)

Operational capabilities consistent with features and requirements that are typical of current and evolving state-of-the-art public safety systems.

Second R&O Para 405

Operational capabilities consistent with features and expectations specified by the public safety broadband licensee that are typical of current and evolving state-of-the-art public safety systems (such as connection to the PSTN, push-to-talk, one-to-one and one-to-many communications, etc.).

B. PSST Network Services and Applications Expectations

1) Public safety should have access to the full suite of current and continually evolving commercial services and applications hosted on the SWBN.
2) All approved PSST-hosted and/or other third party public safety applications and services will be delivered via the SWBN, consistent with specified performance, network transport, and routing parameters.
3) There will be mechanisms for monitoring SWBN adherence and conformance to specified service quality and performance standards, including:
    a. Creation of service level agreements (SLAs) and associated key performance indicator (KPI) definition, metrics, and reporting.
    b. KPIs measured will be limited to the list in Table II-A.
    c. SLA conformance oversight and management; and
    d. SLA violation and shortfall identification, notification, and correction.
4) The D Block winner should provide agreed-upon services-related SLA reports to the PSST, as well as access to the source data for such reports:
    a. Monthly KPI/SLA compliance reports indicating compliance against SLAs;
    b. Access to service assurance systems and data to perform analysis on compliance and out-of-compliance situations and remedies; and
    c. Formal quarterly reviews of performance against NSA SLA agreements between the PSST and the D Block operator
5) Originally published in the NPSTC Broadband Working Group's Statement of Requirements (SoR),[2] Table II-B provides a list of applications and services that should be supported on the SWBN. Parameters such as delay, delay variation, throughput, etc, in addition to the stipulated KPI's for such applications and services, will be negotiated in the NSA.

[2] Public Safety 700 MHz Broadband Statement of Requirements

Table II-A Key Performance Indicators

Key Performance Indicator	Abbreviation
Availability(Service)	Av(S)
Accessibility(Service)	Ac(S)
Access Time(Service)	AT(S)
End to End Delay(Service)	EED(S)
Access Delay(Service)	AD(S)
Release Failure	RF(S)
Time to Restore	TTR
Grade of Service (Service)	GOS(S)
Bit Error Rate	BER
Latency(Service)	Latency(S)
Jitter	Jitter
Event Notification	EN
Response Time	RT
Continuity of Service Connections	CSC
Quality of Sessions	
System Responsiveness	
One-Way Transmission Delay	
Payload Content Preservation	
% Packet Mis-Direction per Session	

Table II-B Applications and Services

Application/Service	**Description**	**Data Rate**
File transfer	*i.e.* to download such items as high-resolution images, GIS data, etc.	Greater than 256 kb/s
Email		Less than 16 kb/s
Web browsing		Greater than 32 kb/s
Cellular voice	Analogous to today's cellular system capability.	4-25 kb/s
Push to talk voice	Analogous to commercial offerings, but coupled with group call capability.	4-25 kb/s

Application/Service	Description	Data Rate
Indoor video	Indoor video is video that is transmitted from inside a building, whether it is surveillance or tactical video.	20-384 kb/s
Outdoor video	Outdoor video is video that is transmitted from the street, whether it is surveillance or tactical video.	32-384 kb/s
Location services	This includes location services for personnel as well as vehicles and other objects that public safety tracks.	Less than 16 kb/s
Database transactions	This includes remote databases (data that is not under the agency's direct control) as well as databases that are local.	Less than 32 kb/s
Messaging	Instant messaging and SMS type services, both one-way and two-way.	Less than 16 kb/s
Operations data	This is a catch-all for data that deals with the operations and maintenance of the network, *i.e.* over-the-air programming, remote client management, etc.	Less than 32 kb/s
Dispatch data	This area primarily covers data as it relates to computer-aided dispatching.	Less than 64 kb/s

Application/Service	Description	Data Rate
Generic traffic	This is a catch all for traffic that doesn't fall within any of the categories described above, and that generates less than 64 kb of data per second.	Less than 64 kb/s
Telemetry	Remote measurement and reporting of information for radio devices, vehicles, etc. Also includes sensors data such as passive chemical detection. Additionally, biometric sensors that require better network performance are also included in this application class.	70-120 kb/s
Virtual Private Networking		Less than 64 kb/s

VIII. Operational Control and Use of the Network

A. FCC Rule

§ 27.1305(2)(h); § 90.1405(2)(h)

Operational control of the network by the public safety broadband licensee to the extent necessary to ensure that public safety expectations are met.

1) Local Public Safety Operational Control

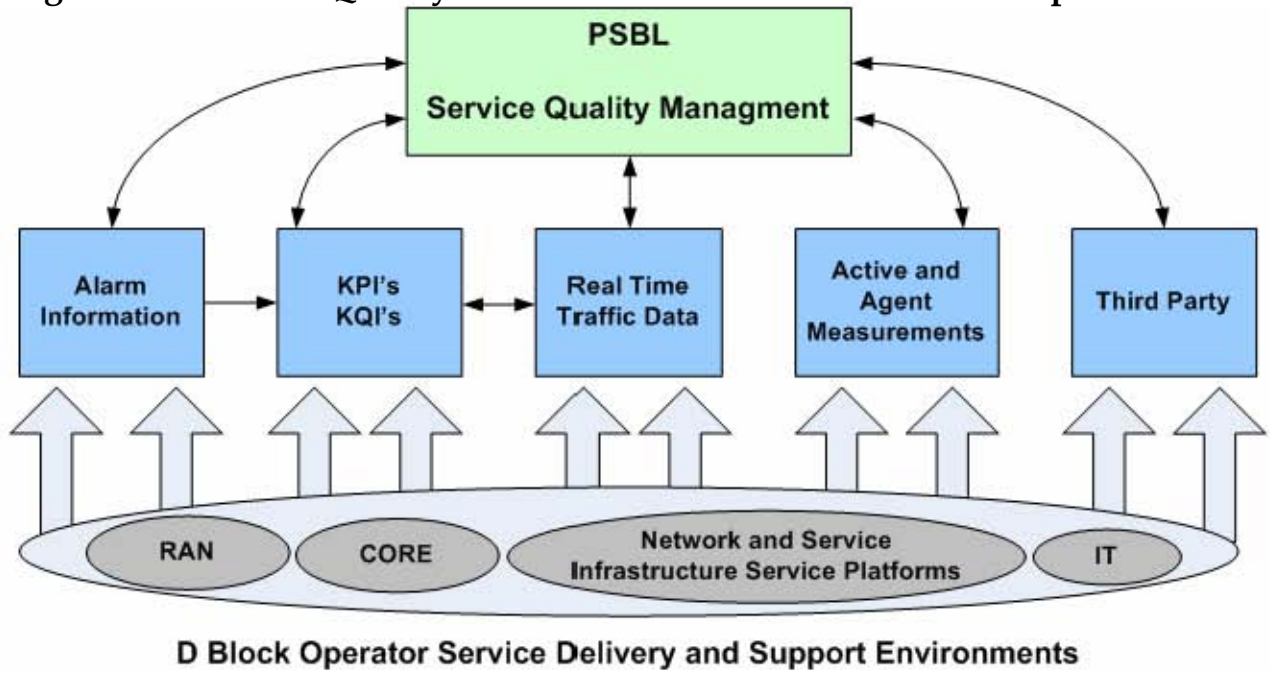
a) Real-time visibility to SWBN network and service quality status relevant to the local agency or jurisdiction. This includes the ability for local public safety users to obtain real-time network status, site status, and access SWBN operator network monitoring system events and alarms for their geographic area. The type, content, source, display, delivery format, security, reliability and other key design parameters will be addressed in the NSA.
b) Real-time access to service management applications with control limited to local agency or jurisdiction SWBN users for them to view and modify user/group/application priorities and profiles, and to add, modify, provision and authenticate priority users and devices.

2) PSST Operational Control

a) The ability by the PSST to host services that may require elements of IP Multimedia Subsystem (IMS) or System Architecture Evolution (SAE) environments for the control and management of services.
b) Physical co-location of trained incident management PSST personnel in the D Block operator's primary and secondary Network Operations Center(s) ("NOCs"). The number of seats and locations are subject to NSA negotiation.
c) Real-time ability to declare an "emergency" for defined geographic area(s), and enable public safety priority and preemption of up to 70% of the engineered capacity for the sites within the emergency location(s).
d) Real-time and near-real-time Operational Support Systems ("OSS") / Network Management Systems ("NMS") visibility to the entire SWBN network and service quality status using the same tools and systems available to the D Block operator.
e) Real-time visibility into public safety consumption of network resources in a given geographic location(s) and real-time alerts/notifications when the priority access capacity maximum of 70% occurs on a given site.
f) To facilitate incidents, the PSST will have access to service management applications with control to setup, modify user/user group/application priorities profiles nationally across agencies and jurisdictions.
g) Additionally, the PSST will have access to service management applications, enabling them to provision or add, manage, and authenticate users and devices nationally across agencies and jurisdictions to facilitate incident management.

h) Access to an over-the-air management framework for managing SWBN public safety user devices (individually or in groups of devices) to clear user data or disable devices.
i) Real-time visibility into malfunctions or failures that impact priority users' services and applications over a wide geographic area of the SWBN.
j) Notification to the PSST of system downtime (or any work that may affect service or system performance) due to planned maintenance, configuration changes, or upgrades. The PSST will provide the D Block licensee with advance notice of planned public safety events to allow time for proper capacity planning and if required, adjustment. The PSST will coordinate with local public safety entities affected by these activities.
k) Figure I sets forth examples of the types of elements to be correlated to provide the level of information by which the PSST can offer oversight and service QoS to its priority users.

Figure I Service Quality Information Flows and Sources Example



IX. Specialized Care and Billing

Although not addressed specifically within the Second Report and Order, public safety has care and billing requirements which are both differentiated and more demanding than the commercial standard provided for consumer and enterprise customers. The PSST lists these requirements for consideration in inclusion in the D Block Service Rules.

A. Specialized Care

The critical nature of public safety's mission requires public safety to have access to specialized care agents in an expedited fashion, with minimal hold time and minimal, if any, automated attendant or Interactive Voice Response system ("IVR") intervention.

D Block specialized care agents interacting with public safety users should be well-trained in the services and applications used by public safety, and should have access to tools providing real-time visibility into public safety personnel services, features, and devices, as well as the ability to modify those services and features real-time in the SWBN and devices.

The PSST recommends that D Block specialized care teams that interact with public safety have NIMS and ICS training to facilitate the integration of D Block care into PSST incident management procedures.

B. Local Agency Self-Care Tools

As discussed in Section VIII, Operational Control and Use of the Network, local public safety jurisdictions and agencies require the ability to access tools securely, which tools provide them with an ability to manage (view, add, delete, change) in real-time their subscribers, services and features, devices and applications, and account information.

Access controls should allow public safety personnel differentiated access to functions and hierarchy levels based upon the users' credentials. As an example, a police chief would have access and control over subscribers within his/her agency, whereas an officer in the same agency would only have access to his/her own profile and services.

C. Specialized Billing

Many public safety agencies have complex departmental accounting, and reporting structures. Billing for public safety requires systems with robust account hierarchy and billing capabilities which can be configured to mirror and support these complex requirements. Key requirements to support public safety accounts and billing include:

1) Hierarchical account structures with a common root account and one-to-many related subordinate accounts (tree structure).

2) Ability to allocate discounts, charges and receivables at different levels within the hierarchy.
3) Multiple (10 or more) sub-account levels within the hierarchy.
4) Sub-accounts at varying levels with distinct invoice, reporting, and receivables allocation configuration.
5) Eligibility validations for agency/jurisdiction orders including:
    a. Established contract (priority access)
    b. Established agency hierarchy
    c. Funds (Purchase Order) availability
6) Product/Pricing catalogs which support mapping to an agency's Contract Line Item Number ("CLIN").
7) Management of multi-period/multi-year Purchase Orders.
8) Multiple invoice formats (electronic, paper, alternate media such as CD-ROM).
9) Equipment-only invoices.
10) Flexible invoice periods (example: monthly, quarterly, yearly).
11) Adherence to OMB Prompt Payment Act (PPA) generally accepted proper invoice recommendations:
    a. Vendor Name
    b. Invoice Date
    c. Payment terms
    d. Contract / PO / Account Number
    e. Detail description of all charges including CLIN

D. Data, Reports, and Analytics

In support of the numerous requirements described in this document for capacity forecasting and service assurance, the D Block operator will require robust data warehouse and business analytics capabilities. Systems must provide for data retention and data details sufficient to achieve the PSST data and reporting requirements. Data envisioned by the PSST to fulfill its functions includes:

1) Public safety user account, subscriber, and service/feature profile data.
2) Public safety usage data.
3) Incident and emergency records and logs.
4) Network event and alarms.
5) Network capacity and utilization statistics.
6) Network coverage data.
7) Public safety application data (subscriptions, usage, event activity).
8) Data is geographically sensitive, must have geographic identifiers allowing for analysis based upon location(s): National, regional (*e.g.,* FEMA regions), state, county, city, township, parish, zip code, cell, sector.
9) Timing and delivery details to be established during NSA negotiation.

E. Support Systems Security

As part of standard operations, the D Block operator should collect and store public safety user identity, contact information, and usage data which could be used to infer

broadband wireless service utilization, location and work patterns for public safety personnel. It is expected that the data security requirements for the D Block operator's back-office support systems may be more stringent than the commercial standard in place for some Business Support Systems ("BSS") and operations. Industry security standards such as PCI, OSI-27001, NIST 800-53 and ITU-T X-805 provide guidance on the physical, logical and application level security and access controls which may be required for the D Block operator's BSS systems and operation.

F. Support Systems Hardening

Some parts of the D Block operator's BSS solution may be involved in providing critical services to public safety. For example, provisioning, self-care, and databases which are part of the BSS solution may become an integral part of emergency incident management tools and procedures. Due to the critical nature of public safety service, components of the BSS platform which are part of a critical service or system will require operational performance and availability SLAs above what is the traditional commercial standard for back-office BSS systems and operations.